ITRM Standard 95-1

Revision 1

June 1, 2000

Commonwealth of Virginia

Information Technology Resource Management Standard

Information Technology Security

DEPARTMENT OF TECHNOLOGY PLANNING

Version: *Basic*
June, 2000

PREFACE

Quick Reference

- Authority
- DTP Review Date
- Definitions
- General Responsibilities
- Effective Date
- Objectives
- Publication Designation
- Purpose
- Scope
- Subject
- Supersedes
- Table of Contents

PUBLICATION DESIGNATION:

CoV ITRM Standard 2000-1 95-1, Revision 1

SUBJECT:

Information Technology Security

EFFECTIVE DATE:

June 1, 2000

SUPERSEDES:

CoV ITRM Standard 95-1: Information Technology Security, Version: Basic (January 31, 1995).

SCHEDULED REVIEW:

One (1) year from effective date

AUTHORITY:

Code of Virginia § 2.1-51.48. - Secretary of Technology
Code of Virginia § 2.1-563.35:3- Department of Technology Planning

Executive Order 51 (99) **-** Department of Information Technology (*Implementing Certain Recommendations by the Governor's Commission on Information Technology*)

SCOPE:

This standard is applicable to all State agencies and institutions of higher education (hereinafter collectively referred to as "State agencies").

PURPOSE:

To define the minimum requirements for the administration of an agency's information technology security program.

OBJECTIVES:

This standard will:

- Define and promulgate the minimum security standards for the protection of the Commonwealth's information technology resources and sensitive information;
- Provide a basis for assisting each State agency in the implementation of minimum standards and prescribe generally accepted security practices; and
- Provide for the compilation of planning material and documentation to support the development of information technology security programs.

DEFINITIONS:

- ***Business Impact Analysis*** is a process that identifies and prioritizes critical business functions. It also includes identifying the resources supporting those functions.
- ***Computer network*** means two or more computers connected by a network.
- ***Confidential information*** is information prohibited from public disclosure that may cause harm to the state, its citizens, or other individuals or organizations.
- ***Contingency Planning*** is the process of creating a plan for emergency response, backup operations, and post-disaster recovery that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation (Synonymous with disaster recovery plan, business continuity plans, and such other designations for plans of this nature).
- ***Critical applications*** are those applications that are so important to the agency that their loss or unavailability is unacceptable.
- ***Critical information*** includes systems and data whose improper use or unavailability could adversely affect the ability of an agency to accomplish its mission.

- ***Custodian*** is the individual or unit responsible for "keeping" the data and the applications and systems supporting it.

- ***Information technology resources*** are specific items such as telecommunications, automated data processing, word processing, management information systems and related equipment, goods, services, and personnel.
- ***Information Technology Security Program*** is the protection of the integrity, availability, and if needed, confidentiality of automated information and resources used to enter, store, process, and communicate it. It is comprised of three groups of security controls: managerial, operational, and technical.
- ***Network*** means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.
- ***Owner*** is the individual or unit who controls the information and determines its level of sensitivity or criticality. As such they determine change, access, dissemination, and update to the data.
- ***Reasonable assurance*** is provided when cost-effective actions are taken to restrict deviations to a tolerable level.
- ***Risk analysis*** is the process of identifying risks, determining their magnitude, and identifying what safeguards are needed.
- ***Risk assessment*** is the results obtained from a risk analysis (Frequently used interchangeably with risk analysis.).
- ***Risks*** are the likelihood or probability that critical applications or confidential or sensitive information will be subject to unavailability, loss, unauthorized modification, or improper disclosure.
- ***Safeguards*** are the protective measures and controls prescribed to meet the security requirements specified for a system. Safeguards may include, but are not necessarily limited to: hardware/software security procedures, operating procedures, accountability procedures, access and distribution controls, personnel security, and physical security.
- ***Sensitive information systems*** contain information, critical or confidential, for which the loss, misuse, or unauthorized access to or modification or improper disclosure could adversely affect the Commonwealth's interest, the conduct of agency programs, or the privacy to which individuals are entitled.
- ***User*** is one who has access to a system.

GENERAL RESPONSIBILITIES:

In accordance with the *Code of Virginia* and *Executive Order 51 (99)*, the following provisions apply:

The Secretary of Technology (SoTECH)

(§2.1-51.47.) establishes *SoTECH as the Chief Information Officer for the Commonwealth. Among the duties assigned are:*

The CIO shall: "Direct the formulation and promulgation of policies, standards, specifications, and guidelines for information technology in the Commonwealth, including, but not limited to, those (i) required to support state and local government exchange, acquisition, storage,
use, sharing, and distribution of geographic or base map data and related technologies"

The Council on Technology Services (COTS)

(§2.1-51.48.) establishes *COTS to advise and assist the SoTECH in exercising the powers and performing the duties conferred by this chapter.*

This standard was developed with the input and concurrence of the COTS.

The Department of Technology Planning (DTP)

(§2.1-563.28:3.) requires the DTP to: *"assist the Secretary of Technology in the development of statewide policies affecting technology at all levels of government, in the business sector, and among the general citizenry., and;*
"5.To review information management plans submitted by agencies and institutions of higher education to the Secretary of Technology. The Department shall recommend to the Secretary of Technology the approval of such plans and any amendments thereto.
6. To monitor implementation of information management plans and periodically reports its findings to the Secretary of Technology.
7. To develop and promulgate policies, standards, and guidelines for managing information technology in the Commonwealth."

The Department of Information Technology (DIT)

*EO-51 (99). D***.** Directs that "DIT shall develop policies and procedures regarding access to state databases and data communications in order to ensure the security of such databases from unauthorized use, intrusion, or other security threats. DIT shall coordinate the implementation of such policies and procedures with agencies maintaining databases hosted outside of the State Data Center."

All State Agencies

Will comply with the SoTECH and DTP policies, standards, and guidelines for managing information technology resources in the Commonwealth.

TABLE OF CONTENTS

SECTION I

EXECUTIVE SUMMARY

The continuing support and involvement of top State agency management is a prerequisite for an effective information technology security program. Management's responsibilities shall include the following:

- Designating an Information Security Officer who administers the information technology security function.
- Determining the optimal place of the security function within the agency hierarchy with the shortest practicable reporting lines to the agency head.
- Approving a business impact analysis, a risk assessment, and continuity plan.
- Facilitating the communication process between data processing managers and those in other areas of the organization.
- Establishing a program of security safeguards.
- Establishing and providing for a security awareness and training program.

The Information Security Officer shall maintain documentation of the agency's information technology security program. It is the vehicle that will be used to communicate the specific procedures needed to implement the security program. It shall contain information on all aspects of the program, including physical security, personnel security, data security, system, and facility access control and communication security.

Documentation shall specify how exceptions to security safeguards should be handled. It shall require the bypass of security safeguards to be completely documented and reviewed by a level of management above that approving the exception to normal procedures.

If any documentation contains sensitive information about agency procedures and safeguards, care shall be taken to ensure that the information is given limited and accountable distribution.

SECTION II

INTRODUCTION

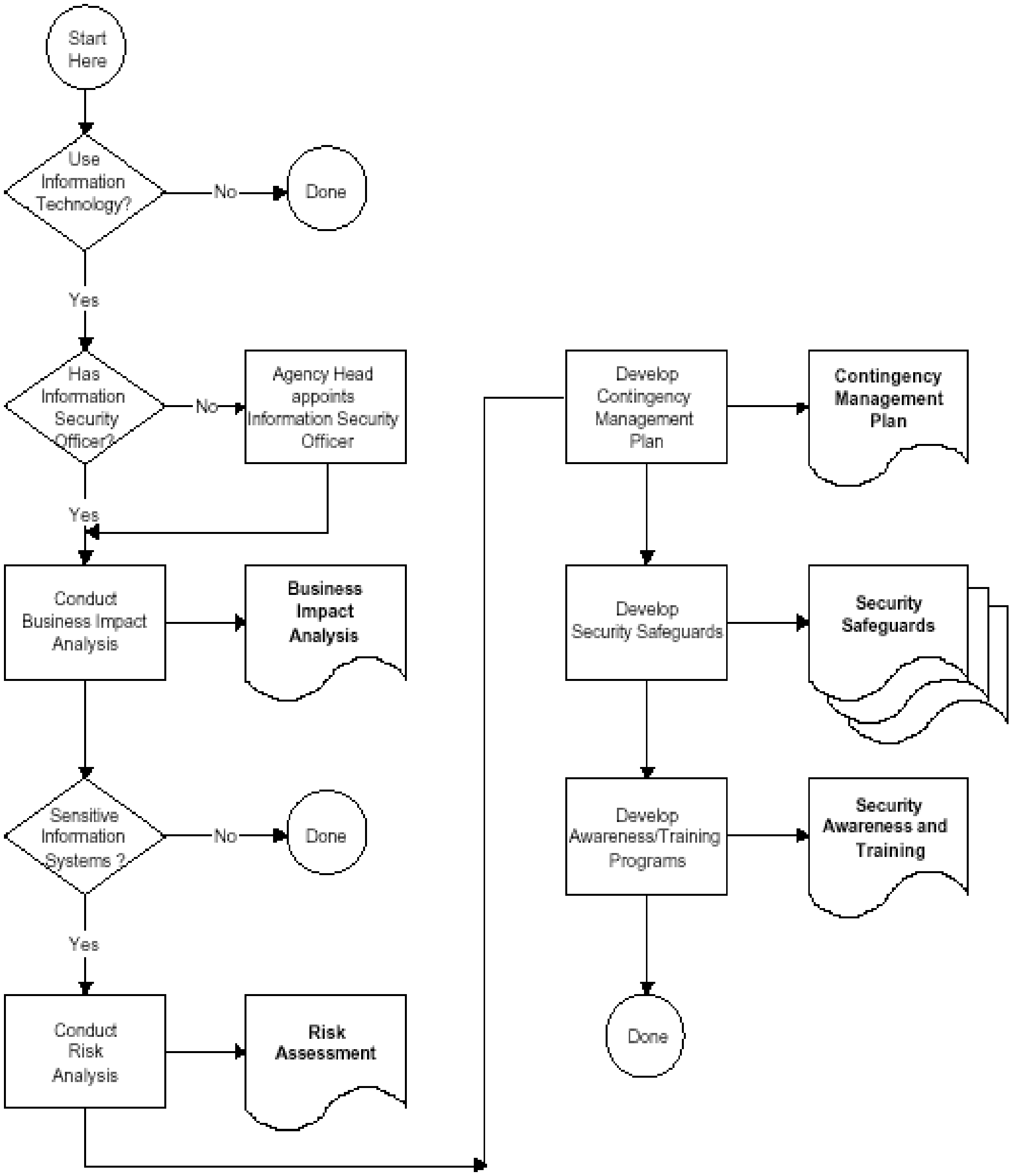
This standard is to be adhered to by State agencies in developing an agency information technology security program consistent with the provisions of CoV ITRM Policy 90-1 (Revised 05/19/95) – *Information Technology Security*..

Each agency will establish, implement, and maintain an information technology security program appropriate to its information technology environment and consistent with State laws, regulations, policies, procedures, and standards. The program must include, at a minimum, adequate and appropriate levels of protection for all sensitive information technology resources within the organization, including hardware, software, physical, and environmental facilities that support information technology systems, telecommunications, administrative, personnel, and data.

Responsibility for the information technology security program begins at the management level and flows down through the agency or institution to the individual user.

- Each agency head is responsible for the security of the agency's information technology resources.
- The Information Security Officer, appointed by the head of each agency, is responsible for implementing and maintaining adequate information technology security programs.
- Owners are responsible for determining adequate and appropriate levels of protection for the information technology resources under their control to prevent unauthorized access or disclosure and to ensure effective and accurate processing and continuity of operations for accomplishment of the organization's mission.
- Custodians are responsible for ensuring adequate and appropriate levels of protection for the information technology resources under their supervision to prevent unauthorized access or disclosure and to ensure effective and accurate processing and continuity of operations for accomplishment of the organization's mission.
- Each employee, including owners, custodians, and users, is responsible for the adequate protection of information technology resources within their control or possession.

The following flowchart is provided as a guide to be used in developing and implementing an agency information technology security program.


Start Here
Use Information Technology?
No
Done
Yes
Has Information Security Officer?
No
Agency Head appoints Information Security Officer
Yes
Conduct Business Impact Analysis
Business Impact Analysis
Sensitive Information Systems ?
No
Done
Yes
Conduct Risk Analysis
Risk Assessment
Develop Contingency Management Plan
Contingency Management Plan
Develop Security Safeguards
Security Safeguards
Develop Awareness/Training Programs
Security Awareness and Training
Done

SECTION III

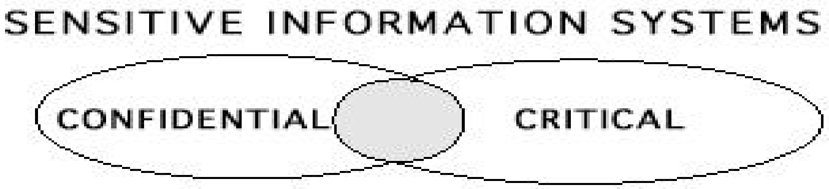
INFORMATION TECHNOLOGY SYSTEM IDENTIFICATION

The security level needed for all information technology systems will be determined based on the criticality of the system and/or the confidentiality of the data processed. The process of identifying an organization's sensitive information systems is called a business impact analysis. The security level of all information technology systems will be identified in one of the following categories:

- Sensitive information systems contain information that requires protection against unavailability, unauthorized access, or disclosure. Sensitive information may be confidential and/or critical:

  Confidential information includes data about individuals requiring protection under the Privacy Protection Act of 1976, proprietary data and data which is not releasable under other applicable laws.

  Critical information includes systems and data whose improper use or unavailability could adversely affect the ability of an agency to accomplish its mission. If the system is required for accomplishment of an agency mission, it need not contain any confidential data to require protection.



- Non-sensitive systems contain data which has no protection required for sensitivity, and the mission of the agency can be accomplished without the system.

Each agency shall conduct a business impact analysis throughout the agency, using a process that will provide reasonable assurance that all information that is potentially sensitive is identified, regardless of where it resides. The business impact analysis will be approved by the head of the agency.

Agencies may use any reasonable and systematic method to determine which information resources must be protected. The result of the business impact analysis should include an estimation of the length of time the agency can continue to function without identified systems.

When there are changes in information technology systems or their environments, the business impact analysis and, if necessary, the risk analysis shall be updated to ensure that appropriate, cost-effective security safeguards are incorporated into existing and new systems.

Agencies must document the results of the business impact analysis. They may identify this information in any way that is sufficiently clear and specific to enable the agency to decide which, and at what level, information technology systems are to be protected.

All systems must include security safeguards that reflect the true importance of the information processed on the system and/or the State's investment embodied in the components of the information technology system.

SECTION IV

RISK ANALYSIS: IDENTIFYING POTENTIAL THREATS

Once the sensitive information technology systems to be protected have been identified through the business impact analysis, the threats to which they are subject shall be evaluated.

The objective of this risk analysis is to provide a measure of the relative vulnerabilities and threats to information resources so that security safeguards can be effectively utilized to minimize the potential for future losses.

Agencies shall establish and implement a risk analysis process for developing a documented risk assessment. The risk assessment shall be approved by the head of the agency.

The risk assessment shall identify additional safeguards that are needed or shall explicitly state that existing safeguards are adequate. Based upon the risk assessment, the agency will develop a program of security safeguards to include documentation on the safeguards to address the defined risks. As described in Section VI, security safeguards address physical security, personnel security, data classification, access control, and communications.

The risk analysis process shall ensure that the balance of risks, vulnerabilities, threats, and countermeasures achieves a residual level of risk that is acceptable, based on the sensitivity of the information technology systems and its impact on the mission of the agency.

The risk analysis may vary from an informal, but documented, review of a microcomputer or terminal installation to a formal, fully quantified risk analysis for a large computing environment.

SECTION V

CONTINGENCY PLANNING

The purpose of preparing for contingencies and disasters is to provide for the continuation of critical business functions (business continuity) in the event of disruptions. The preparation for handling contingencies and disasters is generally called contingency planning or contingency management. A secondary purpose of contingency planning is to minimize the effect of disruptions. Many potential contingencies and disasters can be averted or the damage they cause can be reduced if appropriate steps are taken early to control the event.

Agency management shall ensure the necessary allocation of resources for the development and maintenance of a contingency plan for critical information technology systems for the support of critical business functions.

Agencies shall develop, document, maintain, and periodically test a contingency plan that will provide reasonable assurance that critical data processing support can be continued, or resumed within an acceptable time frame, if normal operations of the system are interrupted. These plans will include adequate coverage of:

- Emergency response procedures appropriate to any incident or activity that may endanger lives, property, or the capability to perform essential functions.
- Arrangements, procedures, and responsibilities, including data backup and offsite storage, to ensure that critical operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time.
- Recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at the primary site, or if necessary, at a new facility, following the destruction, major damage or other interruptions at the primary site.
- Minimally acceptable prioritized level of degraded operation of the critical systems or functions to guide implementation at the backup operational site. The contingency plan must accommodate the established priorities.

The contingency plan for large systems supporting critical agency or institutional functions shall be fully documented. Small systems, such as those located in office environments, may develop a more abbreviated and less formal plan. All plans must be operationally tested at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information processing support.

SECTION VI

SECURITY SAFEGUARDS

The results of the risk analysis and assessment shall be implemented as the agency's Security Safeguards Program. Depending on the agency environment, the following safeguards shall be considered for implementation. All implemented safeguards shall be fully documented and refer back to the risk assessment.

Physical Security

Physical security involves environmental safeguard systems used to protect data processing equipment. It includes normal and emergency operating procedures for fire detection and suppression systems, water detector systems, electric power conditioning equipment, and air conditioning and chilled water supply systems. The existence of an uninterruptible power supply for either graceful power-down or continued operations during an electrical outage is also a significant consideration as a possible security safeguard.

Among the components of physical security are the systems and procedures for controlling physical access to secured data processing facilities.

Physical security may require the participation of several groups outside data processing, including building services personnel, utility suppliers and security personnel.

Personnel Security

Positions should be identified and classified with regard to the sensitivity of the data they control or process and the facilities to which they have access. Pre-employment screening is necessary for persons who will hold sensitive positions, as well as the implementation of procedures for security training activities and procedures for processing terminations, both voluntary and involuntary, of employees in sensitive positions.

Existing state law and regulations impose significant responsibilities on employees for the security of information. State agencies and institutions must comply with such established personnel security policies and procedures.

- The Virginia Employee Standards of Conduct and Performance specifically includes unauthorized use or misuse of state records, falsification of records, the willful or negligent damage or defacing of records and records theft as violations.
- The Virginia Privacy Protection Act of 1976 (Code of Virginia § 2.1-377) specifically requires that State agencies and institutions take affirmative action to establish rules of conduct and to inform employees involved in the design, development, operation or maintenance of an information system that misuse of personal information, or failure to take steps to ensure that information is accurate and reliable, may result in the individual employee being subject to injunction and assessed the costs of court action.

- The Virginia Computer Crimes Act (Code of Virginia § 18.2) imposes both misdemeanor and felony violations for the unauthorized viewing, copying, alteration or destruction of computer data, software or programs.

Data Classification

Data is classified based on the business impact analysis and the risk assessment. The Security Safeguards Program will specify which files and data elements are to be protected, who is assigned their ownership and to what degree protection is to be extended.

Access Control

Access control specifically addresses how agency data is protected and system access is granted. Each agency's Security Safeguards Program shall address how it will control access to agency systems that contain sensitive information. The program should address issues related to the agency's network, hardware platform and application. The program should provide reasonable assurance that sensitive information may be accessed only by authorized users, and should include methods for monitoring and reviewing access to ensure that access controls are functioning as intended.

If a security software package is being used, the installation, implementation and operations of the package must be documented. The security program should separately document the ways this package implements access control for both applications and operating systems facilities.

Communications Security

The complex and highly sophisticated communications networks used with information technology systems require security arrangements specifically tailored to them. These include special physical security provisions, network access control procedures and contingency plans specific to communications networks.

Solutions exist not only to secure each component from the other components, but also to secure the entire network from open networks such as the Internet.

Agencies transporting sensitive information across public networks (e.g., the Internet) should consider encryption to protect it from unauthorized disclosure. Highly sensitive information stored on personal computers, especially laptop computer should be considered for encryption.

SECTION VII

SECURITY AWARENESS AND TRAINING

Agencies with sensitive information systems shall establish and maintain information technology security awareness and training programs to ensure that all individuals involved in the management, operation, programming, maintenance or use of information technology are aware of their security responsibilities and know how to fulfill them.

These individuals shall receive an information technology security awareness briefing or be provided with appropriate information. In addition, employees will be provided with refresher awareness material or briefings as needed.

Individuals assigned responsibilities for information technology security shall be provided with in-depth training regarding security techniques, methodologies for evaluating threats and vulnerabilities that affect specific information technology systems and applications and selection and implementation of controls and safeguards.

The Information Security Officer shall be responsible for documenting and maintaining the security training program.